A Survey on Secure Framework for Privacy-Preserving Over EHR in Cloud Environment

Destin N Joy[1], Chandra Shekhar Yadav[2]

[1]School Of Computer Science Singhania University Pacheri Bari, Jhunjhunu (Raj.), India, Destin.Joy@hotmail.com
[2]Professor and Dean, School of Computer Applications, Affiliation - Noida Institute of Engineering and Technology Greater Noida, csyadavrp@gmail.com ; drcsyadav@niet.co.in

The "Health Service Provider (HSP)" sector is set to be revolutionized by the advent of an emerging technology referred to as "Cloud Computing (CC)". CC's numerous upsides include adaptability, minimal costs, collaborative resources, and rapid implementation. With both individuals and HSPs, the centralized management of data with the cloud creates several confidentiality and safety problems. In addition to shifting control over data to the "Cloud Service Provider (CSP)", data centralization enhances the chances for hackers to gain possession of documents and monitor data when it passes. As a result, both the individual and HSP are at risk of private information being compromised. As a consequence, the widespread acceptance of CC is slowed by issues about integrity, safety, performance, and flexibility. A thorough and methodical analysis of the security and "Privacy-Preserving (PP)" problems associated with HSP systems is presented in this article, along with several PP strategies to guarantee the privacy and security of "Electronic Health Records (EHRs)" within the cloud. This study discusses the difficulties and potential avenues for further research regarding EHR security. Several articles were researched, studied, and analyzed to identify the following areas: cloud-based architecture for EHR, cloud privacy and security necessities for EHR, and different "Cryptography", "Non-Cryptography", and "Biometric" techniques for EHR. It has been observed that the most recent technologies only partially address these issues. In addition, it looks over a few important concerns as well as the many chances for cutting-edge research on EHR security and privacy. A comprehensive approach that strikes a balance between all the conflicting needs is thus critically required.

Keywords: Cloud Computing, EHR, Privacy-Preserving, Security, Cryptographic Approaches.

1. Introduction

Massive advancements in technological innovation at the turn of the millennium are altering the global HSP environment. A sector-wide breakthrough is going to occur in HSP when records on paper have been systematically replaced by EHRs. These innovations improve HSP's effectiveness and capacity for adaptation by establishing a framework for the effective sharing of EHRs across multiple groups of stakeholders.

EHRs have been digital medical records that are routinely accessed and managed by medical professionals, individuals, or family members. This data includes a broad range of details on patients, including their past medical history, demographic data, medications, vaccination status, results of tests performed in laboratories, and other confidential data. Many advantages exist with EHR systems compared to more traditional manual records. It takes shorter periods, energy, and space to store EHRs than traditional copies.

EHRs provide several benefits, such as more accurate decision-making for patients, faster and simpler accessibility of medical information, greater security for patients, less expensive healthcare, and more efficient clinical processes. Over 90 percent of HSPs across Australia are utilizing EHR solutions to help with effective hospital management and clinical scheduling.

Numerous "Cloud Users (CUs)" have verified and attested to EHRs' capability for delivering improved HSP administration. Although "E-Health Cloud (EHC)" offers many advantages over traditional healthcare structures, it also introduces new risks to patients' right to autonomy and the integrity of their medical records.

The HSP sector is heavily using CC, an emerging concept within technology for digital communication. On top of it all, it makes it simple for different HSPs to transmit or interchange EHR data and offers handy storage of health information. In this era of enormous data, where health records are being shared on a massive scale, cloud infrastructures are becoming more important for storing and making accessible vast quantities of data online.

Regardless of time or location, it makes it easy for all parties involved such as HSPs, physicians, and patients to create, save, and retrieve EHR information. When it comes to the efficient and comprehensive retrieval, storage, handling, and amending of EHR data, CSPs deliver tremendous advantages at a reasonable cost. The EHR framework is vulnerable to infiltration or tampering because it functions on a vast network of distant "Cloud Servers (CSs)" that are interconnected and managed as one environment, with various CUs accessing it from many different places.

Furthermore, as most EHRs are very private and critical, storing them on external CSs inevitably raises security risks. Multiple HSPs, including family physicians, physical therapy experts, and insurance companies covering various dental, medical, vision, and other services, are common for patients. An improved, safe, productive, and successful method of distributing and obtaining EHRs across stakeholders is urgently required due to the vulnerable condition of EHRs within the public sector.

Problem Statement: Security and confidentiality of data remains an increasingly important issue within the HSP sector, even though EHRs face several threats related to unapproved accessibility and discretion. Threats range from virus assaults, that hinder EHR privacy and credibility, to "Distributed Denial-of-Service (DDoS)" attempts, that could disrupt the network's ability to deliver rapid medical care to patients. There are far-reaching consequences of intrusions like ransomware that extend beyond economic damage or invasion of privacy. Attackers across the United States gained possession of a significant amount of EHRs, which included the "Social Security Numbers (SSNs)" of over one million individuals, after breaking down the HSP server of a well-known healthcare organization. Similarly, in another instance, the online criminal movement Anonymously crippled HSPs by launching a DDoS assault on the official websites of many hospitals. The urgent necessity of ensuring the anonymity, secrecy, accessibility, reliability, and integrity of EHRs has recently been brought into focus by these instances. Given the potential economic, political, social, and psychological effects of unauthorized possession of EHR data, cyber defense plays a crucial part in recognizing, avoiding, and responding to such incidents. Protecting the privacy of patients' EHRs remains an obligation of HSPs under the "Health Insurance Portability and Accountability Act (HIPAA)". While there are several methods currently under operation to protect HSP platforms in CC environments, hardly any of these methods are reliable.

Paper Contribution: There is no way to guarantee 100% safety for EHC with the current PP technologies. Insider assaults by individuals with approved identities to gain entry to data inside HSPs pose the most serious threat to EHRs stored in CSPs, according to common perception. This is far more serious than attacks from the outside since it involves hackers who are either administrators of databases or key superiors. The purpose of this research is to present a comprehensive analysis of the current security and PP procedures in EHC settings, taking into consideration how these systems leave EHRs open to CC-related vulnerabilities. EHR database includes an extensive range of confidential and private details, ranging from medical files to banking information (such as SSNs and payment card numbers). Its disclosure violates an individual's most basic right, the privilege of privacy in addition to exposing private information about patients and resulting in monetary damages. Throughout this article, it takes a look at the present state of "Cryptography", "Non-Cryptography" and "Biometric" techniques, evaluating their benefits and limitations as well as the issues under consideration. It then suggests an alternative perspective that attempts to address some of these problems while simultaneously establishing a foundation for effective EHR privacy along with effective PP.

Paper Organization: Following the introduction in Section 1, Section 2 covers the recent works that are published in reputed journals, Section 3 details the EHC’s Benefits, Limitations, security requirements, and methodology used by the existing "Cryptography", "Non-Cryptography", and "Biometric" techniques, Section-4 provides the overall discussion of reviewed techniques with its limitations and benefits, and the conclusion of this study and its potential implications for the future are discussed in Section 5.

2. RELATED WORKS

To improve the safety of EHR systems in EHC, the researchers of conduct a qualitative evaluation and provide an alternative based on many technologies, including "Cryptography" and "Block Chain (BC)". Additionally, the article details the obstacles and privacy vulnerabilities that are present in the current systems' databases of EHRs. When it comes to EHRs, cryptography acts as an effective and reliable method for protecting confidential information. An in-depth investigation of the current systems is being carried out to identify the characteristics that have been leading the current EHC platforms to experience significant delays or failures during deployment. Following the review's considerations, an approach had been presented that might be capable of removing the parts of the current models that are failing.

Conventional data safety concepts and processes need to be reevaluated in light of the new privacy, confidentiality, and security challenges presented by EHRs, according to the researchers. The "E-Healthcare Genre-4.0" developed from the "E-Healthcare Genre-1.0" due to the widespread use of IT solutions within HSP. "E-Healthcare Genre-1.0" relied heavily on doctors' and nurses' written records to document patients' health histories. The practice of using EHRs as an alternative to paper documents began during the "E-Healthcare Genre-2.0" initiative. A primary focus of "E-Healthcare Genre-3.0" was providing patients with a means to maintain and access their own EHR information. "E-Healthcare Genre-4.0" has been around for a while, and recently it has evolved to include CC along with "Internet-of-Things (IoT)" to share data with a select group of collaborators. Concerns regarding security for EHC have recently come to light with the fast development of the IT industry within HSP. These issues and the ways to fix them are covered in this article.

To provide a thorough explanation concerning what EHRs are along with why they must be protected, the researchers in conduct a review of the literature. Expand upon the ways that "Internet-of-Medical Things (IoMT)" equipment helps to populate those EHRs with records. In addition, the article explains why EHRs are preserved as "Big Data (BD)". This study also examines the frequently employed security approaches for EHRs. The article concludes by discussing the several performance assessment measures intended to assess EHR.

To establish EHRs and enhance their confidentiality and safety, the researchers of conducted studies using BC innovation. The cryptographic methods and decentralized nature of the BC system could enable it to regulate accessibility to data. This additionally intends to maintain accessibility to data and security at a reasonable level. This study uses electronic agreements to manage the complex parts of the EHR process. Multiple industries, including shipping and accounting, might be part of a network-wide HSP service. It may be enhanced with a web-based application to make it more interactive. EHRs allow chemists to keep tabs on medicinal purchases by allowing them to join the system's database as users.

As part of their literature study, the researchers in examined articles published in "IEEE", "Science Direct", and "Frontier". Researchers go over the many applications of EHR, their developments, pros and cons, safety precautions through BC, usage of both organized and unorganized information, and potential future developments. The characteristics impacting its acceptance, the creation of freely available EHR systems, along with its implementation in crises for refugees as well as shorter or longer travels or healthcare camps are also covered in the article. Furthermore, it highlighted the significance of wearable technology in EHR systems, specifically about improved operations and more economical means of data collecting, collaborating, and analysis. This article concludes by outlining the benefits and drawbacks of EHR systems, as well as their potential future applications.

3. METHODOLOGIES

3.1 Overview of EHC

EHC incorporates digital procedures and interaction with healthcare in a new and innovative way. An organized compilation of a patient's digital medical record is called an EHR when used in an EHC system. EHRs include all pertinent information about patients, such as socioeconomic factors, health history, prescriptions, test results, x-ray images, payment details, and other information that may be considered confidential. When it comes to inexpensive preservation, handling, and amending data through improved quality and effectiveness, the EHC provides outstanding support for all HSPs along with "Data Owners DOs)" similarly. This EHR information has been kept in several CSs, which means it may be accessed on request by DOs as well as CUs virtually anytime. While EHR systems provide many benefits, such as instant, reliable, and upon-request accessibility to patient information, improved treatment quality, and a lower rate of medical mistakes, they also put patients at risk of privacy breaches due to incorrect permission and exploitation of their data. Consequently, several parties' safety and confidentiality concerns are paramount whenever it comes to collecting or exchanging EHR information.

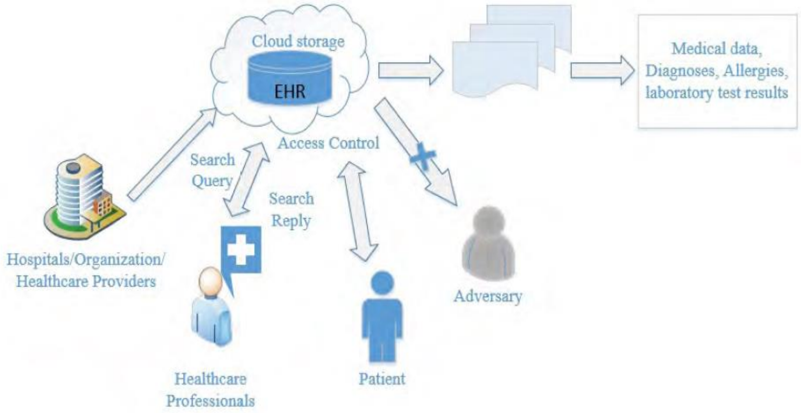

Figure 1. EHC Architecture

Figure 1 shows an overview of the EHC architecture. Based on the data saved, EHC architectural types may be "Public," "Private," "Hybrid," or "Community". Due to the sensitive nature of patient information included in EHR data stored in external healthcare platforms, it becomes essential that appropriate controls for access must be put in place.

3.1.1 Advantages of EHC:

(i) Better treatment for patients: As a result of the patient's ongoing engagement with many HSP professionals. Information about patients may be accessed by medical professionals regardless of time and from any location.

(ii) Savings on costs: It is unnecessary to invest in costly computer software and hardware. Costs associated with buying software and hardware for use on-premises, as well as those associated with providing ongoing maintenance and support, might be eliminated.

(iii) Reduced energy consumption: Due to the elimination of on-site servers and the associated high cooling costs, the power consumption will go down.

(iv) Reliable continuity in the event of a disaster: Nearly every CSP provides a secondary infrastructure with amenities in the event of an emergency.

(v) Researches: For national health studies, illness management, and pandemic inspection, the EHC serves as a centralized information repository.

(vi) Addressing the issue of limited resources: Discussions may be conducted by doctors in distant places using videoconferencing.

(vii) Quick deployment: Quick and easy usage of both hardware and software systems is possible.

(viii) Availability of data: Medical professionals, health centers, care facilities, and insurance firms are merely some of the HSP stakeholders who have permission to use the data.

3.1.2 Limitations of EHC:

(i) Consistency and accessibility: The reliability of broadband connectivity determines the pace at which intermittently, or completely the service is available. The customer service they receive will be significantly impacted by this.

(ii) Flexibility in collaboration: Standards are necessary to ensure that the many HSP platforms can communicate, coordinate, and work together effectively.

(iii) Safety and confidentiality: Loss of information and exploitation are more likely to occur in a public and shareable setting.

(iv) Governing documents: A regulatory, legislative, and moral framework is necessary for the widespread use of CC.

(v) Minimal agency and adaptability: Due to centralized management, there is minimal control over who owns what data. It may be difficult to lease specialized software since most EHC programs remain general.

(vi) Attack susceptibility: A wide range of security threats may compromise the EHC.

3.2 EHC Security and Privacy Requirements

Numerous security standards must be met by CC programs to increase confidence in this innovative technology. The following are the most critical EHC privacy and security demands:

(i) Confidentiality of Data: Making sure that EHRs have been kept hidden from people who are not authorized is known as "Confidentiality". Since the EHR has been made available to a broader range of stakeholders, the possibility of EHR violations increases when data governance is delegated to the EHC. Risks to EHR vulnerability have grown in recent years as the assortment of stakeholders, gadgets, and programs has expanded. Patients need to have faith in the HSP to keep their EHR confidential for the doctor-patient connection to be successful. Encryption and control of access methods could be used to maintain confidentiality.

(ii) Integrity of Data: Integrity guarantees that the EHR that an EHC maintains or makes available to any organization is precise, following the data envisioned, and unaltered. There must be guarantees of high service dependability when employing the cloud for applications that are mission-critical such as EHC. The data and services provided by EHC have to be void of errors. Patients' health might be severely compromised due to incorrect treatment given according to inaccurate data. Similar to non-healthcare usage, HSPs require services that handle EHR data to use checksums or hashes to ensure the data's authenticity and integrity before accessing it. An error message and program termination before processing data are required if an integrity verification fails inside an HSP program.

(iii) Availability of Data: Constant availability of EHRs is critical for the effectiveness of any HSP's EHC system. When it comes to the EHC framework, data availability in emergency scenarios is a significant but sometimes ignored feature. That means being able to keep running in the event of a security compromise or whenever certain officials act inappropriately. In the case of an interruption in power, malfunctioning hardware, infrastructure update, or denial-of-service threat, a highly available system needs to be able to keep services running smoothly. Enforcement of HIPAA privacy and security regulations should not compromise the practicality of EHRs.

(iv) EHR Ownership and Privacy: In most cases, the definition of the DO is the individual who created the data. To safeguard EHR data from abuse or unlawful access, it is essential to determine what insights privileges are provided by the DO. Confidential EHR systems could be created by combining cryptography and watermarked approaches. All parties participating in the possession or development of the EHR must agree before the EHR may be communicated, obtained, or delivered. DOs may decide whether or not other doctors can see their EHRs. Patients can grant permission for certain CUs to access their EHRs within an HSP platform depending on the CU's function or qualities.

(v) CU Authenticity: The genuineness of one's beginnings, credits, promises, and aspirations is what is meant by authenticity in context. This verifies the identity of the entity seeking access. An authenticating procedure is a necessary component of HSP platforms for verifying the identity of entities utilizing the details given by HSPs. Many organizations employ a mixture of passwords and login credentials to protect their users' data against unique threats like "Man-in-the-Middle (MiM)" hacks. For organizations to protect themselves against MiM assaults, almost all encryption protocols provide destination authentication in a particular manner. It is important to verify the identity of CUs including the EHRs provided by HSPs within an HSP platform during each entry point.

(vi) Non-repudiation: Concerns about repudiation arise when CUs, upon obtaining EHR data, dispute the legitimacy of their signatures. As an example, according to the HSP circumstances, following the EHR has been stolen, both the patients and the physicians can dispute the legitimacy of their signatures. Digital certificates and cryptography may be used by EHC programs to prove legitimacy and non-repudiation, much as in e-commerce.

(vii) Freshness and Remanence of Data: The term "Data Remanence" describes the remaining representation of EHR data after it has been officially wiped or eliminated. An inadvertent breach of information confidentiality might be caused by "Data Remanence". Without taking EHR "Data Freshness" into account, the integrity and confidentiality of data within the HSP platform remain insufficient. For data to be considered "Fresh", the EHRs must also be current. Particularly in urgent cases, EHR inconsistencies arise from storage lags and the transmission of obsolete alerts.

(viii) Unlinkability: Unlinkability was an acronym used to describe a CU's repeated utilization of resources or interesting objects lacking the ability to allow additional CUs or individuals to be linked together with their utilization. Accordingly, the attacker's viewpoint remains unchanged about the likelihood of these components having been linked before as well as following their observation.

(ix) Multi-tenancy Cloud: The primary motivations for the development of EHCs had been the potential benefits of pooled computation, storage, and memory. To make the most of their resources whilst keeping expenses down, CSPs use multi-tenancy to be an accepted norm. Therefore, managing accessibility to data and ensuring safe EHR linkage and communication are both afflicted by security vulnerabilities. Secured multitenancy requires that EHRs be physically separated from one another.

3.3 Techniques Currently Employed for EHC Security

Current security techniques employed for establishing EHC security must be discussed following the needs of EHR privacy. "Cryptography," "Non-Cryptography," and "Biometric" constitute the three distinct classifications of techniques employed.

3.3.1 Techniques Using Cryptography

A definition of "Cryptography" is a method by which one may change the format of significant information into something meaningless and then return it to its original version by employing the same key. Several approaches employ multiple techniques for encrypting data and decryption; examples include "Symmetric-Encryption (SE)", "Asymmetric-Encryption (AE)", and "Attribute-Based Encryption (ABE)" techniques.

Secure data transmission, authenticating CUs and information, permission for CUs, and non-repudiation are all made easier by this Although every one of these methods employs a unique set of characteristics and a wide range of approaches to guarantee the safety of sensitive information, the following are the specific methods and their applications in the field of EHC research:

(i) SE Techniques:

The initial factor is that the "Secret-Key Encryption (SKE)" method employs the same SK over both the encryption of data and its decryption Policies, responsibilities, and accessibility rights associated with every CU constitute a few of the unique privileges. Following that, when employing the SKE technique, every one of these requirements must be satisfied concerning the administration of SKs, whereby the SKs and their accessibility permissions are delivered to the specifically approved CUs. When it comes to EHC, "Advanced Encryption Standard (AES)" represents the SKE technique all software uses.

When it comes to EHC SKE techniques, NIST recommends AES because of the incredibly quick and safe it has prove.

The researchers of suggested an SKE method that takes advantage of the AES approach; in this procedure, several SKs have been employed to partly encrypt the file's contents, and the DO assigns various SKs for every CU based on their function. Furthermore, the researchers of recommend employing selected AES, an upgraded version that outperforms its predecessor AES in both performance and safety. In this case, the recommendation states that data compression should occur before AES encryption, through the CU choosing an SK length from a range of "(128,192,256)".

According to the researchers of, a personalized AES within DaaS, a service provided by the cloud, renders it quicker as well as more efficient whenever combined with BD, hence it's suggested to employ it in combination with BD within EHC systems. Implementing SKE enhances the security of the EHR; nevertheless, when trying to meet the demands of the EHC's Role-based decryption, either reconfiguration to include SKE or the implementation of a system to regulate accessibility related to it will become necessary.

(ii) AE Techniques:

The subsequent phase is to put into practice the AE or "Public-Key Encryption (PKE)" techniques, which employ two keys: a "Public-Key (PuK)" is used for encrypting data, and a "Private-Key (PrK)" key is used for decrypting data. "Elliptic Curve Cryptography (ECC)" and "RSA" constitute the two most often employed algorithms for encrypting data within EHC. To accomplish fine-grained encryption of files, a single authentication strategy employing RSA is to divide CUs across different categories, such as "Admin," "Patient," "Doctor," and "Hospital". Following that, specific EHRs associated with every category undergo encryption employing RSA.

As per the context provided in reference, the secured EHR documents have been preserved in a multilayer repository containing the PrK when employing RSA inside the HSP repository. According to this idea, every CU is allowed to access their profile, through which they can obtain the PrK as well as decryption the EHR documents, depending on their database access level. The researchers of highlighted ECC as a further AE method that has been suggested for EHR security due to its computing benefit compared to existing linearity techniques.

The researchers of examined the efficiency of ECC with RSA upon the relevant system; the results suggested that ECC was quicker due to its application of a reduced key length while still maintaining an adequate degree of security. The usage of a combining mechanism specifically designed for decryption and encryption of information has been employed in conjunction with ECC, as described.

A CU identification chip, a "Smart-Card Reader", a "USB Controller", and a "Wireless Transmitter" make up an integrated module. The USB is connected to a wireless gadget through a USB interface which transports data through the radio transmitters. Using an "Identity-Based Encryption (IBE)" framework, the researchers of achieved the ability to regulate who may access EHRs, simplify the handling of keys, and protect against "External", "Equation", and "Reverse" threats in the context of CC.

The researchers of demonstrated the privacy and efficiency of an upgraded "Identity-Based Proxy Re-Encryption (IBPRE)" method and an improved IBE with deployment in EHC platforms. Additionally, they declared their IBPRE technique is less expensive for DOs and CUs that perform re-encryption more effectively, thereby protecting EHR information.

(iii) ABE Techniques:

The final sort of cryptography is known as ABE, and it uses a specific property for encrypting the EHR, then has to correspond to the CUs for its decryption. There are two variants of ABE, an extension of PKE cryptography. First was "Ciphertext-Policy ABE (CP-ABE)" which ties each deciphertext to its corresponding approach, while another was "Key-Policy ABE (KP-ABE)" which reverses the key-ciphertext relationship on its side. This is why ABE is a vital component of EHR platforms; it allows for "Fine-Grained Access Control" and "Role-based Decryption" of openly accessible EHR, indicating that irrespective of how many approved CUs have possession of a specific item of information, only those who meet the criteria for key construction have the ability and decryption and review the EHR documents. Because of these features, it satisfies the security standards for EHCs.

To facilitate the creation of the encryption-key as well as the encrypting ehr information, the researchers of constructed a library of software that comprises both CP-ABE and KP-ABE, as well as a policy generation for producing ABE regulations. According to the researchers employed "Multi-Authority ABE (MAABE)" to construct ABE by dividing CUs among domains. Each domain has comparable powers, which makes the handling of keys easier.

To securely exchange EHR information, the researchers of employed a "Fine-Grained" and "enhanced MA-ABE (eMA-ABE)" method. This architecture guarantees the privacy of data and the ability to revoke CUs if needed. Finally, an environment with hybrid characteristics may make utilization of one or more of the various sorts of techniques outlined before.

Combining many cryptography methods, such as "Proxy Re-encryption" along with the "Asymmetric-Key Encryption" approach, is advantageous for hybrid networks. Digital signatures generated by RSA enable CU authorization while encrypting information using AES guarantees the confidentiality and privacy of EHRs and thus is a form of fused cryptography. In general, a hybrid framework is a good choice since it takes the benefit of several sets of policies at once, which may lead to improved privacy, and faster processing while reducing expenses, electronic signatures, and accessibility privileges.

3.3.2 Techniques using Non-Cryptography

Previously mentioned above is the significant role that cryptography plays in ensuring the safety within the EHC platform. Still, several different approaches towards security that do not rely on cryptographic techniques. Although these techniques contribute some protection to EHC, it's fail to be nearly enough to warrant their widespread usage because cryptographic methods provide much higher levels of security. Hybrid architectures combining these types of systems with cryptographic approaches are therefore used. The following is a list of several non-cryptography techniques:

(i) AAM Techniques:

The "Authentication and Access-Control Manager (AAM)" concept is among such methods. It involves the EHC storing EHRs along with the CS authenticating CUs and determining who has access rights. When dealing with complicated calculations, this framework depends on the EHC. A further approach involves establishing a "Central Authority (CA)" that grants CUs accessibility to, shares with, and manages EHRs for CUs classified as "Patients", "Doctors", "Nurses", "Family", or "Insurance Companies" among other security categories. This approach is in charge of distributing encryption keys and achieving CU rights of entry and CU authenticity using the application of security levels that provide varying levels of permission for CUs.

(ii) RBAC Techniques:

The researchers achieved positive aspects that include "Role-Based Access Control (RBAC)" in addition to the implementation of policies utilizing the adoption of "Extensible Access Control Mark-up Language (XACML)". It's a hybrid of "Extensible Mark-up Language (XML)" along with "Attribute-Based Access Control (ABAC)"—in alongside to constructing an XML representation of their EHRs. Because of RBAC's shortcomings, the researchers suggested a two-tiered approach for access management that combines RBAC on the initial layer and a revised RBAC at the following layer. While the revised RBAC controls the amount of data per CU, the RBAC decides who may view the service that was requested. The following layer is schedule-centered and keeps the patient's appointment schedules, that is distinctive per each individual.

The researchers of presented an EHC-based "Privacy-Aware RBAC" paradigm that may be used to manage and monitor EHRs and approve accessibility to EHR services. The researchers also deserve recognition for their innovative approach, which they termed "Certificate-Based Encryption with Keyword Search (CBEKS)". An AE method is used to execute this procedure. The recipient of the data must first transmit a keyword describing the required data package followed by a certificate expressing the permissions for access to establish the appropriate access privileges. Regarding EHR distribution within EHC frameworks, the researchers employed a searchable and PP method called "Dynamic SE with Keyword Range Search and Multi-Keyword Search (DSEKRSMS)" in conjunction with a "PPEquality-Test (PET)".

(iii) BC Techniques:

Reducing the duration of EHR evaluation was suggested by combining the "Fully-Private BC (FPB)" and "Consortium BC (CB)" models into a single "BlockChain (BC)" architecture. In this case, FPB serves as the traditional repository for HSPs, whereas CB stores the EHRs of each stakeholder. The space that it offers is both dependable and impermeable to tampering.

A patient-centered EHC framework was evaluated by the researchers as a privately managed EHR framework that makes utilization of BC innovation. This framework allows for the verification of the DO of the patient's information, and the granting of access rights, including the assurance of data security. An EHC platform using multi-tier BC architecture with a protocol called "Pseudonym-Based Encryption and Different-Authorities (PBEDA)" was suggested in to meet the requirements of distributed architecture. Since all operations performed on outsourcing EHRs constitute a transaction, BC operates to safeguard them against illicit changes. Effective control of access mechanisms for secured, decentralized information preservation and distribution was suggested by the researchers employing BC in conjunction with collaborative "Inter-Planetary File System (IPFS)" storage.

3.3.3 Techniques Using Biometrics

Numerous organizations are currently employing biometrics since it gives each individual a distinct identification. Authentication of users and recognition are two services offered by biometric techniques. The "Minutiae-Map" method verifies the CU's identity based on their fingerprint traits, which constitutes one biometric authentication method for EHC. Compared to the "Gabor Feature", "Orientation Maps", and "Orientation Co-linearity" techniques, it is easier and faster to acquire fingerprint features, and it also has a higher safety rating. Regarding storing providers, the suggested method divides the CU's EHR data into two separate cloud-based storage accounts, "Cloud Me" and "Dropbox". The RC4 technique has been employed for encrypting the files.

Web-based applications network firewalls, cookies data safeguards, and CU input verification checks are among the methods for preventing "Cross-Site Request Forgery (CSRF)" and "Cross-Site Scripting (XSS)" threats Secure EHR information exchange and accessibility is made possible by the biometric technology described, which makes use of both a patient's identifier and their thumb imprint. The researchers of set up a plan to ensure the safety of health tracking programs that collect data from patients' biosensors; this strategy secures the information at rest and keeps the EHR safe whenever it's within the cloud. Secured patient-doctor interaction across an unsafe open network is possible with the help of the "Multi-Factor Remote User" protocol suggested. The technique employs a hybrid of biometric identification, electronic gadgets, and credentials to safeguard CU identification.

4. DISCUSSION OF THE STUDY

This study has previously covered several security techniques employed to protect EHC platforms; now it will discuss the benefits and drawbacks of such techniques with the objective that researchers could speculate on how to improve these in future endeavors. Considerations such as actual-time data accessibility, EHR availability, and proper and unmodified transmission of EHR between the origin to the terminal are important when attempting to prevent undesired disclosure of EHC information, which might directly impact the life of the patient.

Based on these standards, the cryptographic methods work well. On the other hand, EHC cryptography has a few issues that have been brought to light. In the early stages, the SE is safe, quick, and may provide adequate protection. Unfortunately, this SE strategy lacks RBAC privileges, which means that an additional mechanism for regulating personal information accessibility or two-step encryption, that adds complexity, cannot be implemented together. One way to fix this is by making this method faster to calculate or modify it to ensure it fits the EHC criteria.

Similar to the SKE, the PKE is challenging. Nonetheless, it has other potential uses, including a digitally signed mechanism and key distribution across different CUs. The major issue occurs when a CU is removed from an EHC framework, this necessitates modifying all of the framework's rules regarding access, regardless of whether the ABE structure has the capability of granting RBAC rights.

Methods that are not dependent on encryption are more efficient and take less time to implement. Employing physiological characteristics for CU authorization and authentication, biometric technologies work well. Cryptography methods, in general, are less efficient than non-cryptography methods, regardless of how much safer the former may be. Using non-cryptography methods in combination is better than using techniques for cryptography alone.

To address this issue along with offering a desired privacy system, a hybrid approach employing cryptography, non-cryptography, and biometric approaches may be implemented. The most suitable approaches to protecting the EHC, corresponding to this overhaul of the articles cited, might include an elaborate AES that has different CU categories, numerous levels of privileges, and minimal expense, an ABE alongside an effective CU rejection approach, an RSA with appropriate control over access and an enhanced application of fingerprint compatible using mobile gadgets, or a hybrid that combines "Non-Cryptography", "Biometric", and "BC" techniques.

According to the findings of this study into EHC security concerns, it seems that might be wise to look at biometric mechanisms for mobile gadgets and BC-based mechanisms, the latter of which have been getting a lot of attention recently. The RSA-based approach for the ABE-based hybrid architecture deserves to be considered by those interested in cryptography methods for protecting the EHC platform.

When designing a system for security, it is possible to consider a few of the unresolved issues about EHC security, such as how to handle crises, how to distribute keys efficiently, and how to revoke CUs in conjunction with changing the EHC system's accessibility policies. These areas might potentially host future EHC studies. This evaluation stands out from others on the subject of the safe EHC platform as it explored the whole literature for the most pertinent information. With the addition of biometrics to the already-established cryptography and non-cryptography methods, security techniques may be classified into three broad groups. The benefits and drawbacks of various security techniques, including cryptography, non-cryptography, and biometric authentication methods, are also given in Table 1.

Table 1: Advantages and Disadvantages of Reviewed Techniques

Types of Techniques	Advantages	Disadvantages
Cryptography Techniques	• Sharing keys has strong security that is role-oriented. • Enhanced security and performance with role-based encryption. • Secure encryption of files with granular control. • Enhanced data accessibility with less effort and time spent on it. • Enhanced security and access rights are provided. • The system's scalability has become improved.	• An increase in both the quantity of keys and the complexity of key administration. • Compressing data is an essential first step before encryption. • Because of BD, scalability is restricted. • It is necessary for managing the accessibility model. • Control over access with several levels is necessary. • The overhead associated with computation is incurred. • Modifying one's accessibility rights is a challenging task.
Non-Cryptography Techniques	• Lowers the CU's time spent on online commitments. • Authorization and access to user privileges are guaranteed. • Offers a means of accessibility regulation that is centered on attributes. • The CUs' permissions for access have been determined. • Provides clients with platform protection. • Quickens the process of validating data.	• Using a semi-trusted CS, all calculations are executed. • Supervision by a centralized authority is essential. • Overhead in computation. • For enhanced safety, additional studies on BC innovation are required. • There is still no effective solution to the link-ability issue, which hinders effective search. • To remove fraudulent downloads, the Data-Pushing mechanism is missing.
Biometric Techniques	• Allows for the safe storing, retrieval, and recognition of CU data. • Protects information while making it simple to access and share. • A higher degree of privacy protection is implemented. • Cost of communication reduced.	• Could be vulnerable to further hacking attempts. • Contrary to handheld electronic gadgets.

5. CONCLUSION

This article accumulates, from a variety of sources, a large body of literature on the topic of EHC system security. This article provides a concise overview of the several security measures utilized by EHC platforms to ensure the safety of EHR storage and exchange over the cloud. The techniques discussed include "Biometrics", "Non-Cryptography", and "Cryptography". There are additionally hybrid structures that take into account aspects of many techniques. The last part provides a concise overview of the benefits and drawbacks of certain security solutions that have been used. Future research could utilize the constraints as a starting point for developing a more robust security mechanism that was possible with earlier iterations of the technology. In addition to this, several methods, including "BC", "Biometrics", "ABE", "AES", and "RSA", are put forward, as well as a collection of articles that other scholars likely employ to build standards of security for the EHC platform. Integrating security regulations into the framework and using sophisticated bio-inspiring encryption methods are also areas that might be explored in future studies to improve the privacy and safety of EHR systems.

References

1. Brotherton, T., Brotherton, S., Ashworth, H., Kadambi, A., Ebrahim, H. and Ebrahim, S., (2022). "Development of an Offline Open-Source Electronic Health Record System for Refugee Care", Front Digit Health, 4. DOI:10.3389/fdgth.2022.847002
2. Maarsingh et al., (2022) "Implementing electronic health records on a medical service trip improves the patient care process", Frontiers in Health Services, 2. DOI:10.3389/frhs.2022.960427
3. Mehrtak, M. , SeyedAlinaghi, S., MohsseniPour, M., Noori, T., Karimi, A., Shamsabadi, A., Heydari, M., Barzegary, A., Mirzapour, P. Soley-manzadeh, et al., (2021) "Security challenges and solutions using healthcare cloud computing", Journal of Medicine and Life, 14 (4), 448. DOI: 10.25122/jml-2021-0100
4. Ari, A. A. A., Ngangmo, O. K., Titouna, C., Thiare, O., Mohamadou, A., Gueroui et al., (2020) "Enabling privacy and security in cloud of things: Architecture applications security & privacy challenges", Applied Computing and Informatics. DOI:10.1016/j.aci.2019.11.005
5. Sharma, D. S., Chakravarthi, A. A., Shaikh, A. A. A., Ahmed, S., Jaiswal and Naved, (2021) "The aspect of vast data management problem in healthcare sector and implementation of cloud computing technique", Materials Today: Proceedings.
6. Dhaya, R., Kanthavel and Venusamy, (2021) "Dynamic secure and automated infrastructure for private cloud data center", Annals of Operations Research, 1-21. DOI: 10.1007/s10479-021-04442-0
7. Sonkamble, S. P., Phansalkar, V. M., Potdar and Bongale, (2021) "Survey of Interoperability in Electronic Health Records Management and Proposed Blockchain Based Framework: MyBlockEHR", IEEE Access, 9, 158367-158401. doi: 10.1109/ACCESS.2021.3129284
8. Al Mamun, S., Azam and Gritti, (2022) "Blockchain-Based Electronic Health Records Management: A Comprehensive Review and Future Research Direction", IEEE Access. doi: 10.1109/ACCESS.2022.3141079
9. Nirmala, B. K, and Christi N. A, (2022) "A Review on Cloud Cryptography Techniques to Improve Security in E-health Systems," 2022 6th International Conference on Computing Methodologies and Communication (ICCMC), Erode, India, 100-104, doi: 10.1109/ICCMC53470.2022.9753999.
10. Talati, R. and Chaudhari, P., (2022) "The Road-ahead for E-healthcare 4.0: A Review of Security Challenges," 2022 1st International Conference on Informatics (ICI), Noida, India, 208-213, doi: 10.1109/ICI53355.2022.9786917.
11. Sharma, D. and Prabha, C. (2023) "Security and Privacy Aspects of Electronic Health Records: A Review," 2023 International Conference on Advancement in Computation & Computer Technologies (InCACCT), Gharuan, India, 815-820, doi: 10.1109/InCACCT57535.2023.10141814.
12. Ansari, M. F., Dash, B., Swayamsiddha, S. and Panda, G. (2023) "Use of Blockchain Technology to Protect Privacy in Electronic Health Records- A Review," 2023 International Conference on Intelligent Data Communication Technologies and Internet of Things (IDCIoT), Bengaluru, India, 144-149, doi: 10.1109/IDCIoT56793.2023.10053417.
13. Thakur, S., Gupta, B., Mathur, U. and Bansal, D. (2023) "Electronic Health Record Systems for Enhanced Medical Care: A Survey," 2023 International Conference on

Intelligent Systems for Communication, IoT and Security (ICISCoIS), Coimbatore, India, 257-262, doi: 10.1109/ICISCoIS56541.2023.10100356.

14. Rezaeibagha, F., Win, K. T., & Susilo, W.(2015). A systematic literature review on security and privacy of electronic health record systems: technical perspectives. Health Information Management Journal 44(3): 23-38. DOI: 10.1177/183335831504400304
15. Sumathi, R., & Kirubakaran, E. (2013).SCEHSS: Secured Cloud-Based ElectronicHealth Record Storage System with Re-Encryption at Cloud ServiceProvider. International Journal of Computer and Communication Engineering 2(2): 162. DOI:10.7763/IJCCE.2013.V2.161
16. Omotosho, A., &Emuoyibofarhe, J. (2015). A criticism of the current security, privacy and accountability issues in electronic health records. arXiv preprint arXiv:1501.07865. DOI: 10.5120/ijais14-451225
17. Varsha, B. S., &Suryateja, P. S. (2014). Using Advanced Encryption Standard for Secure and Scalable Sharing of Personal Health Records in Cloud. International Journal of Computer Science and Information Technologies (IJCSIT) 5(6): 7745-7747.
18. Oh, J. Y., Yang, D. I., & Chon, K. H. (2010). A selective encryption algorithm based on AES for medical information. Healthcare informatics research 16(1): 22-29.
19. Shin, D., Sahama, T., &Gajanayake, R. (2013, October). Secured e-health data retrieval in DaaS and Big Data. In Proceedings of 2013 IEEE 15th International Conference on e-Health Networking, Applications and Services (Healthcom 2013) (IEEE), 255-259. doi: 10.1109/HealthCom.2013.6720677.
20. Abbas, A., & Khan, S. U. (2014). A review on the state-of-the-art privacy-preserving approaches in the e-health clouds. IEEE Journal of Biomedical and Health Informatics, 18(4), 1431-1441. doi: 10.1109/JBHI.2014.2300846
21. Ramakrishnan, N., &Sreerekha, B. (2013). Enhancing Security of Personal Health Records in Cloud Computing by Encryption. In International Journal of Science and Research (IJSR). https://www.ijsr.net/archive/v4i4/SUB152944.pdf
22. Pooja, Batra, N. (2014). Secure Mechanism for Medical Database Using RSA. International Journal of Application or Innovation in Engineering & Management 3(7): 320-327.
23. Dhanabagyam, S. N., and G. R. Karpagam. (2017) Secure Communications for e-Health in Mobile Cloud Computing Using Provable Security. International Journal of Pure and Applied Mathematics 114(7): 325-335. https://acadpubl.eu/jsi/2017-114-7-ICPCIT-2017/articles/7/31.pdf
24. Sridevi, R., &Nithiya, C. (2016). E-Health Security using ECC algorithm. International Journal of Advanced Research in Basic Engineering Sciences and Technology (IJARBEST), 2(19): 114-117. https://ijarbest.com/index.php?option=com_login&task=download_volume_doc&id=877&fname=spcl18&ftype=conference
25. Tsai, K. L., Leu, F. Y., Wu, T. H., Chiou, S.S., Liu, Y. W., & Liu, H. Y. (2014). A Secure ECC-based Electronic Medical Record System. J. Internet Serv. Inf. Secur. 4(1): 47-57. https://jisis.org/wp-content/uploads/2022/11/jisis-2014-vol4-no1-05.pdf
26. Liu, C.H., Lin, F.Q., Chiang, D.L., Chen, T.L., Chen, C.S., Lin, H.Y., Chung, Y.F., and Chen, T.S., (2013) Secure PHR access control scheme for healthcare application clouds. In proceedings of 2013 42nd International Conference on Parallel Processing, (IEEE), pp. 1067-1076. doi: 10.1109/ICPP.2013.127
27. Wang, X. A., Ma, J., Xhafa, F., Zhang, M., & Luo, X. (2017). Cost-effective secure E-health cloud system using identity based cryptographic techniques. Future Generation Computer Systems 67: 242-254. Doi: 10.1016/j.future.2016.08.008.
28. Rezaeibagha, F., Win, K. T., & Susilo, W. (2015). A systematic literature review on security and privacy of electronic health record systems: technical perspectives. Health Information Management Journal 44(3): 23-38. DOI: 10.1177/183335831504400304

29. Akinyele, J. A., Pagano, M. W., Green, M. D., Lehmann, C. U., Peterson, Z. N., & Rubin, A. D. (2011, October). Securing electronic medical records using attribute-based encryption on mobile devices. In Proceedings of the 1st ACM workshop on Security and privacy in smartphones and mobile devices (ACM), 75-86. DOI:10.1145/2046614.2046628
30. Kulkarni, K., & Dixit, A. M. (2014). Privacy Preserving System Using Attribute Based Encryption for e-health Cloud. https://www.ijsr.net/archive/v3i12/U1VCMTQzODE=.pdf
31. Selvam, L., &Arokia, R. J. (2018, March). Secure Data Sharing of Personal Health Records in Cloud Using Fine-Grained and Enhanced Attribute-Based Encryption. In Proceedings of 2018 International Conference on Current Trends towards Converging Technologies (ICCTCT) (IEEE), 1-6. doi: 10.1109/ICCTCT.2018.8551006
32. Sadikin, M. A., &Wardhani, R. W. (2016, July). Implementation of RSA 2048-bit and AES 256-bit with digital signature for secure electronic health record application. In proceedings of 2016 International Seminar on Intelligent Technology and Its Applications (ISITIA) (IEEE), 387-392. doi: 10.1109/ISITIA.2016.7828691
33. Kahani, N., Elgazzar, K., & Cordy, J. R.(2016, April). Authentication and access control in e-health systems in the cloud. In proceedings of 2016 IEEE 2nd International Conference on Big Data Security on Cloud (Big Data Security), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS) (IEEE), 13-23. doi: 10.1109/BigDataSecurity-HPSC-IDS.2016.43
34. Liu, C.H., Chen, T.L., Lin, H.Y., Lin, F.Q., Liu, C.M., Wu, E.P., Chen. T.S. (2013) Secure PHR Access Control Scheme in Cloud Computing. International Journal of Information and Electronics Engineering 3(3):329. doi: 10.1109/ICPP.2013.127.
35. Drozdowicz, M., Ganzha, M., & Paprzycki, M. (2016). Semantically enriched data access policies in eHealth. Journal of medicalsystems 40(11): 238. DOI:10.1007/s10916-016-0581-7
36. Lu, S., Hong, Y., Liu, Q., Wang, L., & Dssouli, R. (2007, November). Access control in e-health portal systems. In proceedings of 2007 Innovations in Information Technologies(IIT) (IEEE), pp. 88-92. DOI:10.1109/IIT.2007.4430378
37. Chen, L., & Hoang, D. B. (2011, September).Novel data protection model in healthcare cloud. In proceedings of 13th IEEE International Workshop on FTDCS 2011, the International Conference on ATC 2011, the 8th International Conference on UIC 2011and the 13th IEEE International Conference on HPCC 2011, September 2, 2011 -September 4, 2011 (IEEE), 550–555. doi: 10.1109/HPCC.2011.148.
38. Gritti, C., Susilo, W. & Plantard, T. (2016). Certificate-based encryption with keyword search enabling secure authorization in electronic health record. Journal of Internet Services and Information Security, 6 (4): 1-34. https://jisis.org/wp-content/uploads/2022/11/jisis-2016-vol6-no4-01.pdf
39. Xu, C., Wang, N., Zhu, L., Sharif, K., & Zhang, C. (2019). Achieving Searchable and Privacy-Preserving Data Sharing for Cloud-Assisted E-healthcare System. IEEE Internet of Things Journal, 6(5): 8345-8356. doi: 10.1109/JIOT.2019.2917186
40. Han, H., Huang, M., Zhang, Y., & Bhatti, U. A. (2018, June). An architecture of secure health information storage system based on blockchain technology. In proceedings of International Conference on Cloud Computing and Security (Springer, Cham), 578-588. https://api.semanticscholar.org/CorpusID:52312930
41. Chenthara, S., Ahmed, K., Wang, H., & Whittaker, F. (2019). Security and Privacy-preserving Challenges of e-Health Solutions in Cloud Computing. IEEE Access, 7: 74361-74382. doi: 10.1109/ACCESS.2019.2919982.
42. Badr, S., Gomaa, I., & Abd-Elrahman, E. (2018). Multi-tier blockchain framework for IoT-EHRs systems. Procedia Computer Science, 141: 159-166.

https://doi.org/10.1016/j.procs.2018.10.162

43. Cao, S., Zhang, G., Liu, P., Zhang, X., &Neri, F. (2019). Cloud-assisted secure eHealth systems for tamper-proofing EHR via blockchain. Information Sciences, 485: 427-440. DOI:10.1016/j.ins.2019.02.038
44. Nguyen, D. C., Pathirana, P. N., Ding, M., & Seneviratne, A. (2019). Blockchain for Secure EHRs Sharing of Mobile Cloud-based eHealth Systems. IEEE Access, 7: 66792-66806. doi: 10.1109/ACCESS.2019.2917555.
45. Vinodhini, A. N., &Ayyasamy, S. (2017, March). Prevention of personal data in cloud computing using bio-metric. In proceedings of 2017 International Conference on Innovations in Green Energy and Healthcare Technologies (IGEHT) (IEEE), 1-6. doi: 10.1109/IGEHT.2017.8094085.
46. Gopal, G.V., and Saiphani, K.V., (2017). Providing security with biometric system to the health data using cloud storage. International Journal of Recent Trends in Engineering & Research, National Conference on Convergence of Emerging Technologies in Computer Science and Engineering (CETCSE-2k17), 266-272. DOI:10.23883/ijrter.conf.20171201.054.y4tpd
47. Sharma, S., & Balasubramanian, V. (2014, November). A biometric based authentication and encryption framework for sensor health data in cloud. In Proceedings of the 6th International Conference on Information Technology and Multimedia (IEEE), 49-54. doi: 10.1109/ICIMU.2014.7066602.
48. Albarki, I., Rasslan, M., Bahaa-Eldin, A. M., &Sobh, M. (2019). Robust Hybrid-Security Protocol for HealthCare Systems. Procedia Computer Science, 160: 843-848. https://doi.org/10.1016/j.procs.2019.11.001